UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/648,555	08/25/2003	Stuart Cain	200310064-1	5177

22879 7590 12/27/2007

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
WYSZYNSKI, AUBREY H	
ART UNIT	**PAPER NUMBER**
2134	

NOTIFICATION DATE	DELIVERY MODE
12/27/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
mkraft@hp.com
ipa.mail@hp.com

Office Action Summary	Application No.	Applicant(s)	
	10/648,555	CAIN, STUART	
	Examiner	Art Unit	
	Aubrey H. Wyszynski	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 September 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *1-9* is/are allowed.

6)☒ Claim(s) *10-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *25 August 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 9/19/07 has been entered.

2. Claims 1-20 are pending.

Response to Arguments

3. Applicant's arguments, with respect to claims 1-9 have been fully considered and are persuasive. The rejection of claims 1-9 has been withdrawn.

4. Applicant's arguments with respect to claims 10-20 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 10-20 rejected under 35 U.S.C. 103(a) as being unpatentable over Cohen et al., US 6,952,779 above, and further in view of Szor, US 2005/0022018.

Regarding claims 10 and 13, Cohen discloses a security intrusion mitigation system comprising:

a means for communicating information;

a means for processing information including instructions for determining a highest risk path that has the highest risk of an attack spreading between network components included in said highest risk path in comparison to risks of attacks spreading between network components associated with other risk path (fig. 1, illustrates a flow diagram showing a method of detecting and analyzing risks in a computer network; fig. 1, #140 ranks the vulnerabilities according to actual risk and ranks the risk level, col. 9, lines 23-43). Cohen lacks or does not expressly disclose automatically mitigating said attack. However, Szor discloses automatically mitigating said attack from spreading between said network components included in said highest risk path ¶[0012], ¶[0021-0023];

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of Cohen with the system of Szor to automatically mitigate an attack from spreading between network components based on the highest risk path in order to defeat malicious code before it becomes widespread on the network, as taught by Szor ¶ [0022].

Cohen further discloses a means for storing said information, including instructions for storing information describing said highest risk path (fig. 3, #225).

Regarding claims 11-12 and 14, Szor further discloses security intrusion mitigation system of claim 10 wherein said instructions include security management instructions implemented on a network application management platform (fig. 1, #112, local analysis center computer system or intrusion detection system #108), a means for centrally controlling a utility data center operations.(fig. 1, #116, global analysis center).

Regarding claim 15, Cohen discloses computer usable storage medium having computer readable program code embodied therein for causing a computer system to implement security intrusion mitigation instructions comprising:
a component risk determination module for determining that a first risk of a first attack spreading from a first component to a second component is higher than a second risk of a second attack spreading from a third component to a fourth component, wherein said first, second, third and fourth components are included in a network fig. 1, illustrates a flow diagram showing a method of detecting and analyzing risks in a computer network; fig. 1, #140 ranks the vulnerabilities according to actual risk and ranks the risk level, col. 9, lines 23-43 and col. 8, line 8-col 9, line-43). Cohen lacks or does not expressly disclose an attack spreading response module. However, Szor discloses an attack spreading response module for responding to said first risk before responding to said second risk ¶[0012], ¶[0021-0023].

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of Cohen with the system of Szor to automatically mitigate an attack from spreading between network components based on the highest risk path in order to defeat malicious code before it becomes widespread on the network, as taught by Szor ¶ [0022].

Regarding claim 16, Cohen in view of Szor further discloses the computer usable storage medium of Claim 15 wherein said first risk is biased based upon an economic value of functions said second component performs (col. 3, lines 20-32).

Regarding claim 17, Cohen in view of Szor further discloses the computer usable storage medium of Claim 15 said first risk is biased based upon connectivity of said second component to said first component in said network (col. 3, lines 40-45 and fig. 5).

7. Claims 18-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cohen in view of Szor as applied to claims 15-17 above, and further in view of Fox et al, US 6,535,227.

Regarding claim 18, Cohen in view of Szor discloses a computer usable storage medium of claim 17. Cohen in view of Szor lacks or does not expressly disclose wherein

said response includes reducing traffic communication to said second component. However, Fox discloses wherein said response includes reducing traffic communication to said second component (col. 12, lines 16- 30). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the device of Cohen in view of Szor with the device of Fox to reduce traffic communication in order to reduce one or more vulnerabilities, as taught by Fox, (col. 12, lines 16-30).

Regarding claims 19 and 20, Cohen in view of Szor discloses a computer usable storage medium of claim 15. Cohen in view of Szor lacks or does not expressly disclose wherein said response includes turning off an interface of said second component to said network. However, Fox discloses wherein said response includes turning off an interface of said second component to said network (col. 12, lines 16-30): It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the device of Cohen in view of Szor with the device of Fox to turn off an interface in order to reduce one or more vulnerabilities, as taught by Fox, (col. 12, lines 16-30)

Allowable Subject Matter

8. Claims 1-9 are allowed.

Conclusion

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aubrey H. Wyszynski whose telephone number is

(571)272-8155. The examiner can normally be reached on Monday - Thursday, and alternate Friday's.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on 5712723811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

AHW

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

12,19,07